(54) Title: RIJNDAEL BLOCK CIPHER APPARATUS AND ENCRYPTION/DECRYPTION METHOD THEREOF
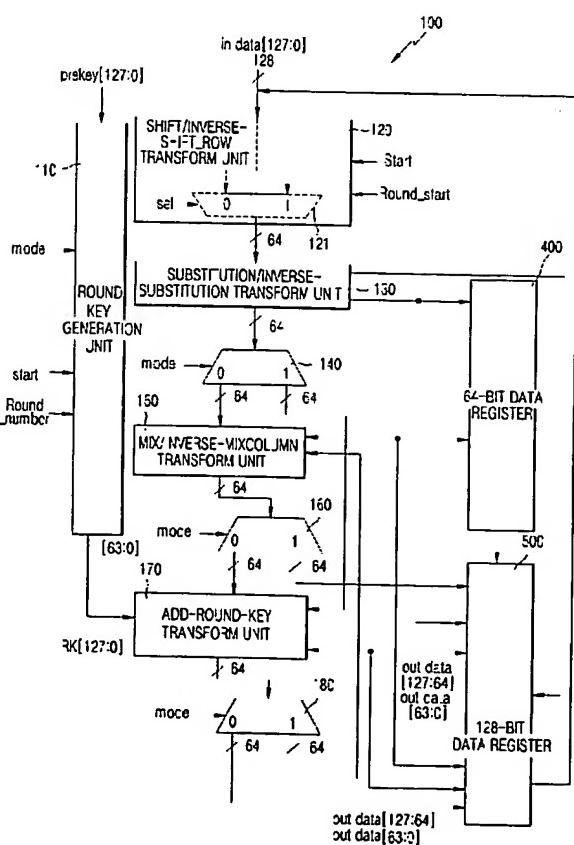
(57) Abstract: A rijndael block cipher apparatus including an op-
erational unit that efficiently performs a round operation for en-
crypting/decrypting a rijndael block cipher and an encryption/de-
cryption method thereof are disclosed. The rijndael block cipher
apparatus is mounted in a mobile terminal such as a cellular phone
and a PDA or a smart card, which requires a high-rate and small-
sized cipher processor, and can encrypt and decrypt important data
that requires security at high speed and perform the round operation
with respect to upper 64 bits and lower 64 bits which are divided
from 128-bit input data. Thus, the cipher apparatus can reduce the
time required for encryption/decryption of the rijndael block cipher
and the size of the apparatus.

KG, KP, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.